UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE NEW YORK TIMES COMPANY, NICHOLAS CONFESSORE, and GABRIEL DANCE, Plaintiffs, - against - FEDERAL COMMUNICATIONS COMMISSION, Defendant.	:	18 Civ. 8607 (LGS)

REPLY MEMORANDUM OF LAW IN FURTHER SUPPORT OF PLAINTIFFS' CROSS-MOTION FOR SUMMARY JUDGMENT

David E. McCraw, Esq.
Al-Amyn Sumar, Esq.
The New York Times Company
Legal Department
620 Eighth Avenue
New York, NY 10018
Phone: (212) 556-4031
Fax: (212) 556-4634
mccraw@nytimes.com

John D. Clopper, Esq.
Clopper Law PC
43 West 43rd Street, Suite 95
New York, NY 10036
Phone: (347) 752-7757
jclopper@clopperlaw.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Plaintiffs The New York Times Company, Nicholas Confessore, and Gabriel Dance (collectively, "The Times") respectfully submit this memorandum of law in further support of their cross-motion for summary judgment on their Complaint brought under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552.

PRELIMINARY STATEMENT

In 2017, malicious actors hijacked the FCC's electronic commenting system. The harm was severe. Millions of fake comments were filed in the net neutrality proceeding. Release of the API proxy server log would greatly advance the public understanding of what happened during the net neutrality proceeding. But the FCC continues to resist such a public accounting, grasping at dubious claims that release of the information might possibly cause negative effects on commenter privacy. The FCC's claims dramatically overstate the potential for harm. At best, the FCC has established that release of the server log might—possibly—cause third-party digital advertisers to adjust the advertisements being served to some internet users. And while the FCC hints darkly at the possibility of greater threats to privacy, such as identity theft, it provides no support for this conclusory allegation. In short, the FCC has failed to show that release of the server log "would" result in "a clearly unwarranted invasion of personal privacy."

Finally, the FCC may not withhold the entire server log simply because it contains some entries related to proceedings other than the net neutrality rulemaking. Regardless of whether the FCC is required to search the server log in the manner requested by The Times, the FCC may not withhold the entire log. Agencies may not withhold entire records simply because the records contain some non-responsive information.

I. The FCC Has Failed to Demonstrate That Release of the Server Log Would Result in a Clearly Unwarranted Invasion of Personal Privacy

The FCC both overstates the intrusion on personal privacy that may result from release of the server log and understates the public interest in release of the information. The hypothetical intrusions on personal privacy alleged by the FCC are not the types of privacy interests that Exemption 6 is intended to cover. On the other hand, release of the server log would greatly server the public interest by shedding light directly on the FCC's performance of its statutory obligations.

A. Commenters' Privacy Interests in IP Addresses and User-Agent Header Information Are Negligible

The FCC has failed to meet its burden of demonstrating that commenters have a substantial privacy interest in either the IP addresses or the User-Agent header information contained in the server log. With respect to IP addresses, the FCC's argument fails for two reasons: (1) the FCC fails to demonstrate, as required by Exemption 6, that the harm is certain to occur; and (2) the claimed harm—the use of IP addresses to serve digital advertisements—is fleeting and insubstantial. With respect to User-Agent header information, FCC has utterly failed to support its claim; its declarations are wholly conclusory and unsupported.

1. The FCC Has Failed to Demonstrate Release of IP Addresses Will Definitely Cause a Privacy Intrusion

The FCC has fallen far short of meeting the requirements of Exemption 6, which permits withholding of information only if release of the information "would" result in a "clearly unwarranted invasion of personal privacy." As the Supreme Court has stated, "Exemption 6 was directed at threats to privacy interests more palpable than mere possibilities." *Dep't of Air Force v. Rose*, 425 U.S. 352, 380 n.19 (1976); *Carter v. U.S. Dep't of Commerce*, 830 F.2d 388, 391

(D.C. Cir. 1987) (stating that "[w]ithholding information to prevent speculative harm" is contrary to the FOIA's pro-disclosure policy).[1]

Here, the FCC has repeatedly conceded that the putative threat to privacy is a mere possibility—the FCC claims only that it is *possible* that online advertisers *might* be able to make use of some of the data in the server log to serve targeted advertisements to individual internet users. *See* Dkt. 23, Defendant's Memorandum of Law ("FCC Memo") at 19 (referring to "*substantial possibility*" of harm); *id.* at 19 (stating release "*can* constitute an unwarranted invasion of personal privacy"); *id.* at 20 (malicious actors "*could* use this information" to harm); *id.* (malicious actors "*can potentially* exploit" the information); *id.* at 21 (stating disclosure of IP addresses "*could* result" in invasion of personal privacy); Dkt. 24, Declaration of Erik Scheibert, dated March 14, 2019 ("First Scheibert Declaration"), at ¶ 37 (malicious actors "*could* use this information" to harm the user); Dkt. 29, Defendant's Reply Memorandum of Law ("FCC Reply") at 3 (discussing "*potential*" harms from disclosure); Dkt. 30, Second Declaration of Erik Scheibert, dated May 2, 2019 ("Second Scheibert Declaration") at ¶ 3 (stating release "*could*" compromise a user's privacy).

These repeated admissions are fatal to the FCC's claim. As another district court recently observed, "the defendant undermines its own claims that the information it has provided satisfies the requirements of Exemption 6 because it asserts that public disclosure of the withheld information 'could' or 'may reasonably lead to' the risks identified, . . . whereas Exemption 6

[1] The standard set forth in Exemption 6—that release of the information "would" cause a "clearly unwarranted invasion of personal privacy"—is notably different from the standard set forth in Exemption 7(C), which permits withholding if disclosure "could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C). *See Nat'l Archives & Records Admin. v. Favish*, 541 U.S. 157, 165-66 (2004); *Am. Civil Liberties Union v. Dep't of Def.*, 543 F.3d 59, 83-84 (2d Cir. 2008), *cert. granted, judgment vacated*, 558 U.S. 1042 (2009).

requires an agency to demonstrate that 'disclosure ... *would* constitute a clearly unwarranted invasion of personal privacy.'" *New Orleans Workers' Ctr. for Racial Justice v. United States Immigration & Customs Enf't*, No. CV 15-431 (RBW), 2019 WL 1025864, at *23 (D.D.C. Mar. 4, 2019) (emphasis added).

Moreover, even if the FCC had not repeatedly conceded the abundant uncertainties that inhere in the potential misuse of the information contained in the server log, those uncertainties are apparent from the record. First, as explained more fully in The Times's opening brief, most individual users connect to the internet using dynamic IP addressing. *See* Dkt. 28, Plaintiffs' Memorandum of Law ("NYT Memo") at 12. Dynamic IP addresses change frequently, and, as a consequence, are far less useful than static IP addresses for purposes of tracking computers over a given period of time. That is especially so here, given that the IP addresses were collected two years ago. The FCC essentially acknowledges this and instead argues that it cannot be certain that the server log does not contain any IP addresses that are still currently in use by individual users. *See* Second Scheibert Declaration ¶ 4. This is precisely the sort of uncertain-to-occur possibility that the courts have held is not sufficient to support withholding under Exemption 6.

Second, unlike many other types of personally-identifying information, such as Social Security numbers, IP addresses identify computers, not people. There is nothing about IP addresses that necessarily link an IP address to a particular internet user. For example, anyone connecting to an open Wi-Fi network—such as in a local coffee shop or other public area—will likely share an IP address.[2] The FCC claims that it is possible that digital advertisers may be able

[2] *See, e.g., In re BitTorrent Adult Film Copyright Infringement Cases,* 296 F.R.D. 80, 84 (E.D.N.Y. 2012) ("Some of these IP addresses could belong to businesses or entities which provide access to its employees, customers and sometimes (such as is common in libraries or coffee shops) members of the public."); *Strike 3 Holdings LLC v. John Doe,* 19 Civ. 20761 (S.D.

to link the IP addresses to individual commenters' identities and other data, such as browsing history, which may, in turn, reveal something personal about the commenters that would not be publicly available absent release of the IP addresses. *See* Second Scheibert Declaration ¶ 5. Maybe so, at least theoretically—but this this is precisely the sort of multi-step speculation that is insufficient to justify withholding information under Exemption 6.[3] *Am. Civil Liberties Union*, 543 F.3d at 85-86 ("[S]peculation does not establish a privacy interest that surpasses a *de minimis* level for the purposes of a FOIA inquiry.").

2. The Harm Cited by the FCC—Targeted Digital Advertising—Is Relatively Insubstantial

Even if the FCC was able to establish that release of the IP addresses "would" result in an intrusion on privacy, the specific harms relied on by the FCC would be not be sufficiently substantial for purposes of Exemption 6. Advertising is, for better or worse, a part of everyday life, both online and offline.[4] While it is possible that release of the IP addresses could theoretically cause digital advertisers to alter the mix of ads that some individual users might see online, this consequence pales in comparison to the types of harms—such as embarrassment,

---

Fla. May 8, 2019) ("There is nothing that links the IP address location to the identity of the person actually [using the computer]."); *Strike 3 Holdings LLC v. Doe*, 329 F.R.D. 518, 522 (S.D.N.Y. 2019) (noting that IP addresses may not link to actual infringer in copyright case).

[3] As discussed in The Times's opening brief, millions of comments were submitted to the FCC during the net neutrality notice-and-comment period. *See* NYT Memo at 3-5, 21. The fact that there are millions of similarly-situated commenters reduces the risk of harm resulting from disclosure of the information contained in the server log. *See New York Times Co. v. U.S. Dep't of Treasury*, No. 09 Civ. 10437 (FM), 2010 WL 4159601, at *6 (S.D.N.Y. Oct. 13, 2010); *Washington Post Co. v. U.S. Dep't of Agric.*, 943 F. Supp. 31, 34 (D.D.C. 1996) ("Indeed, it is precisely because the list is so large and the information so generic that the individual privacy interests are so small.").

[4] *See* Stuart A. Thompson, Opinion, *These Ads Think They Know You*, N.Y. Times (May 13, 2019), https://nyti.ms/2LaIzxD (explaining that digital ads are "powered by vast, hidden datasets").

harassment, and physical safety—that typically warrant withholding of information under the FOIA's personal privacy exemptions. *See, e.g., Perlman v. DOJ,* 312 F.3d 100, 106 (2d Cir. 2002), *vacated & remanded*, 541 U.S. 970, *on remand*, 380 F.3d 110 (2d Cir. 2004) (per curiam); *New York Times Co. v. U.S. Dep't of Treasury*, No. 09 Civ. 10437 (FM), 2010 WL 4159601, at *4 (S.D.N.Y. Oct. 13, 2010).

3. The FCC Has Failed to Adequately Support the Claim That Release of IP Addresses and User-Agent Header Information Will Result in Identity Theft

While the FCC's principal argument is that release of IP addresses might possibly cause commenters to receive different digital advertisements, the FCC also claims that release of the information in the server log might have some marginal utility to bad actors seeking to commit identity theft or other significant harm. *See* FCC Reply at 3. The FCC's declarations on this point, however, are entirely conclusory, stating only that User-Agent header information "can potentially inform malicious actors as to whether the user is employing an outdated browser or an operating system with a vulnerability." First Scheibert Declaration ¶ 37. It appears the FCC believes that the mere mention of identity theft will be considered sufficient to justify withholding the information.[5] As a matter of law, however, it is not nearly sufficient. *See Story of Stuff Project v. U.S. Forest Serv.*, 345 F. Supp. 3d 79, 97 (D.D.C. 2018) ("[An] agency may satisfy its burden of showing a substantial invasion of privacy by affidavits containing reasonable specificity of detail rather than merely conclusory statements.").

[5] Indeed, the risk of harm here is made all the more speculative by the fact that the User-Agent header information contained in the logs is now two years old—a span of time in which most users will likely have updated their browsers and operating systems.

B. Any Incidental Intrusion on Personal Privacy is Greatly Outweighed by the Public Interest in Release of the Server Log

The FCC has not established a cognizable privacy interest in the data contained in the server log. But, if it had, that privacy interest would be far outweighed by the public interest in the information. Because the server log will disclose, for instance, to what degree a small number of IP addresses were used to post comments, its release will help explain how the net neutrality rulemaking was hijacked by Russians and others to create the lie that millions of citizens were demanding that the FCC's net neutrality rules be repealed.

Remarkably, the FCC disclaims any responsibility for how the comment period of the net neutrality proceeding was conducted. *See* FCC Reply at 6 (denying the "purported obligation" to ensure that notice-and-comment is not overrun by fraud). As a matter of basic administrative law, this is wrong. Section 553(c) of the Administrative Procedure Act requires agencies to "give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation." Beyond that, section 553(c) also requires that "[a]fter consideration of the relevant matter presented, the agency shall incorporate in the rules adopted a concise general statement of their basis and purpose." In other words, notwithstanding the FCC's disclaimer, it undeniably has a statutory duty to provide the public a meaningful opportunity to comment on proposed rules and to meaningfully consider the relevant comments presented.[6] Release of the server log will shed light on the FCC's performance of that duty—including, importantly, the consequence of its

[6] It is black letter administrative law that an agency must consider and respond to significant comments received during the period for public comment. *See Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402, 416 (1971); *see also* Statement of Commissioner Jessica Rosenworcel, Dissenting, FCC 18-156, *Memorandum Opinion and Order* (Dec. 3, 2018) https://bit.ly/2HPvBTv (explaining FCC's statutory duties in notice-and-comment rulemaking).

remarkably narrow view of the scope of that duty—by revealing the true extent of the fraud that infected the net neutrality rulemaking and, importantly, the extent to which cloud-based automated bots intervened in an important public debate. Because release of the server log will "serve the core purposes of the FOIA by contributing significantly to public understanding of the operations or activities of the government," *Nat'l Ass'n of Home Builders v. Norton,* 309 F.3d 26, 33 (D.C. Cir. 2002) (alterations and internal marks omitted), the FCC should be ordered to release the log.[7]

II. The FCC Cannot Withhold the Entire Server Log Simply Because It Contains Some Entries Related to Other Dockets

The Times has requested that the Court order the FCC to produce the server log limited to the entries that correspond to the net neutrality proceeding, Docket No. 17-108. *See* NYT Memo at 19-20. The FCC claims that it is not required to undertake this task, incorrectly claiming that The Times has asked the FCC to "perform research" to answer the FOIA request. *See* FCC Reply at 8-9. Rather, The Times is simply asking that its FOIA request be fulfilled by searching the server log for entries related to Docket No. 17-108. *See* NYT Memo at 19-23. While the FCC complains that this will take some effort and a measure of judgment to sort the data, *see* FCC Reply at 10, that is always the case when searching for responsive records.

In any event, to the extent that searching within the server log is unduly burdensome, the appropriate result is to release the entire log—including the entries unrelated to the net neutrality proceeding. The server log unquestionably includes responsive information that The Times has

[7] The district court in *Prechtel v. Fed. Commc'ns Comm'n* got the public interest analysis exactly right. Release of additional information about the comments that were filed in the net neutrality proceeding "would clarify the extent to which the Commission succeeded—as it assured the American people it had—in managing a public-commenting process seemingly corrupted by dubious comments." *Prechtel v. Fed. Commc'ns Comm'n*, 330 F. Supp. 3d 320, 331 (D.D.C. 2018).

requested. The FCC cannot withhold the document because it may contain information that is not responsive to The Times's request. *See Am. Immigration Lawyers Ass'n v. Exec. Office for Immigration Review*, 830 F.3d 667, 677 (D.C. Cir. 2016) ("[O]nce an agency identifies a record it deems responsive to a FOIA request, the statute compels disclosure of the responsive record—i.e., as a unit—except insofar as the agency may redact information falling within a statutory exemption.").

The FCC has failed to show that any portion of the server log—including log entries related to comments posted outside Docket No. 17-108—is exempt pursuant to Exemption 6. The uncertainties inherent in the possible harms potentially flowing from the release of the log entries are the same regardless of whether a particular log entry relates to Docket No. 17-108 or a different docket. And the public interest in understanding the interference in the FCC's electronic commenting system during this time period is sufficient such that any incidental privacy intrusion is not "clearly unwarranted" for purposes of Exemption 6—especially in light of the fact that the percentage of total comments not relating to net neutrality filed during this time period is somewhere between 0.007% and 0.68%.[8] Accordingly, there is no information within the server log that is exempt from disclosure.

Second, in the event that the Court were to find that some entries could be withheld pursuant to Exemption 6, the FCC would not be entitled to withhold the entire log. Rather, the FCC would be required to do what every agency does when faced with a record that contains both exempt and non-exempt information: segregate the exempt information and release the non-

[8] *See* FCC Reply at 10 n. 5 (explaining differing methodologies for calculating approximate number of comments filed outside Docket 17-108). Recent reports indicate that a substantial number of comments intended for Docket 17-108 were incorrectly filed using the docket number for the FCC's earlier net neutrality proceeding, Docket 14-28. *See* John Eggerton, *Net Neutrality by the Numbers*, Multichannel News (March 29, 2018), https://bit.ly/2JxbOJd.

exempt information. FOIA provides that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection." 5 U.S.C. § 552(b). The FCC does not even attempt to argue that any exempt portions would not be reasonably segregable. In any event, it is clear that the exempt portions—if there were any—would be segregable. For example, the non-exempt entries would not be "inextricably intertwined" with exempt entries. *See, e.g., Inner City Press/Cmty. on the Move v. Bd. of Governors of Fed. Reserve Sys.,* 463 F.3d 239, 249 (2d Cir. 2006) ("[I]nformation that is 'inextricably intertwined' with exempt information cannot be disclosed."). Nor does the FCC claim that it lacks the technological capacity to segregate the entries.[9] *Milton v. DOJ*, 842 F. Supp. 2d 257, 259-61 (D.D.C. 2012); *see also Mingo v. DOJ*, 793 F. Supp. 2d 447, 454-55 (D.D.C. 2011). Accordingly, even if some portions of the server log were exempt, the FCC would be obligated to segregate those entries and release the rest.

CONCLUSION

For the foregoing reasons and the reasons presented in its opening brief, Plaintiffs respectfully asks this Court: (i) to deny FCC's motion for summary judgment and to grant Plaintiffs' cross-motion for summary judgment; (ii) to order the FCC to make public within 20 days, pursuant to 5 U.S.C. § 552, the server log; (iii) to award Plaintiffs the costs of this proceeding, including reasonable attorney's fees, as expressly permitted by FOIA, *id.* § 552(a)(4)(E); and (iv) to grant such other and further relief as the Court deems just and proper.

[9] Despite having filed two declarations in this case, the FCC provides no estimate of how much time or effort would be required to segregate the entries in the server log related to Docket No. 17-108. The declarations, however, do make clear that it is technologically feasible to do so. Moreover, the task is presumably easier than the more complicated task of manipulating the multiple logs previously sought by The Times—before the FCC admitted it possessed a single log with all the relevant data. For that more complicated task, the FCC estimated it would take about a week. *See* First Scheibert Declaration ¶ 33.

Dated: New York, NY
May 22, 2019

Respectfully submitted,

By: /s/ David E. McCraw

David E. McCraw, Esq.
Al-Amyn Sumar, Esq.
The New York Times Company
Legal Department
620 Eighth Avenue, 18th Floor
New York, NY 10018
Phone: (212) 556-4031
Fax: (212) 556-4634
mccraw@nytimes.com

John D. Clopper, Esq.
Clopper Law PC
43 West 43rd Street, Suite 95
New York, NY 10036
Phone: (347) 752-7757
jclopper@clopperlaw.com

Attorneys for Plaintiffs